Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Review of the Emergency Alert System	)	EB Docket No. 04-296
	)	

COMMENTS OF MONROE ELECTRONICS, INC.

TABLE OF CONTENTS

I. Introduction

A. Overview

Monroe Electronics, Inc. respectfully provides our comments in response to the Third Further Notice of Proposed Rulemaking (hereafter "Fourth Further Notice"), in the above-captioned proceeding.

Monroe Electronics supports the Commission's efforts aimed at the creation of an advanced interoperable Emergency Alert System (EAS). In many areas, we believe the Commission is contemplating actions that will enable the creation of a secure and reliable next-generation alert and warning capability.

In other areas, however, we respectfully disagree with certain tentative conclusions posted in the Third Further Notice, and urge the Commission to reconsider their stance on several issues identified within this commentary.

In the comments that follow, Monroe Electronics seeks to address many of the questions that the Commission poses in the Third Further Notice. The approach taken is to rely on the company's well-developed technical expertise in conventional EAS and next generation CAP EAS. Monroe Electronics believes that, ultimately it is the local public alert and warning ecosystem – consisting of the emergency management community, working in tandem with local broadcasters, cable operations, and EAS systems manufacturers - that is best positioned to identify the most-detailed network requirements and resulting system parameters of state and local CAP-based public alert and warning safety systems.

B. About Monroe Electronics / Digital Alert Systems

Incorporated in 1954, Monroe Electronics has maintained a position of leading design and innovation in all its products. We have been involved in public alert and warning for over 30 years, providing EBS-related equipment and solutions, including the first EBS-solution to the cable industry in the 1970s. Monroe Electronics is a leading supplier of EAS equipment to the cable television industry, with the majority of cable operations across the US utilizing and standardizing on the Monroe R189 One-Net system.

Via our Digital Alert Systems subsidiary, we have been one of the most innovative suppliers to the broadcast radio and television industries. In 2007, Digital Alert Systems introduced CAP functionality integrated onboard the DASDEC EAS encoder/decoder, more than three years before FEMA adopted CAP as a standard.

Both the DASDEC and R189 One-Net are FCC-certified and have successfully completed the IPAWS conformance process. The first CAP EAS encoder-decoders to have filed a

Suppliers Declaration of Conformity are the Digital Alert Systems' DASDEC for broadcast radio and TV and the Monroe Electronics R189 One-Net for cable TV and IPTV. Both are FCC-certified encoder/decoders CAP capability built-in. The DASDEC provides an all-in-one "drop-in" solution for broadcaster that fully supports the existing EAS, integrates CAP, and provides the option of three on-board radio receivers (AM-FM-WX).

Monroe's executive staff are board members and active participants in the CAP-EAS Industry Group, and active members of the SCTE EAS committee. Our executives have also served on the SBE EAS committee, the FCC Communications Security, Reliability and Interoperability Council (CSRIC) Working Group 5A and the FCC Commercial Mobile Alert Advisory Committee (CMSAAC).

II. Issues Raised in the Third Further Notice

A. Continuing the use of the existing legacy EAS, including the EAS Protocol.

1. We support the continuing use of the existing legacy EAS, including the EAS Protocol, operating alongside the new CAP EAS system.

As noted in our Informal Comments of May 17th 2010, while we and others have delineated some of the deficiencies in the current broadcast distribution system, we still believe the existing legacy EAS provides valuable redundancy to the proposed next generation system. For this reason, the existing legacy EAS should be maintained. In most natural disasters the broadcast medium is the last system standing and is unparalleled in the "one to many" message distribution.

The existing legacy EAS can serve a useful role as a backup to the next generational CAP capability, thereby enhancing a robust, redundant, reliable warning system. While the use of the legacy EAS does not provide the value-added content of CAP – including expanded warning text, as well as potentially other multimedia like graphics – it does in itself still convey the basic alert message content.

However, we must caution that the watering-down of the capabilities and benefits of next-generation EAS in favor of the legacy EAS may not be in the nation's interest. Specifically, we recommend that the Commission adopt rules that allow EAS participants an option of broadcasting the expanded text, audio and multimedia that may be contained in CAP formatted alerts.

We strongly believe that the new Part 11 rules should define acceptability of a multimodal distribution architecture that includes whatever forms of IP dissemination that a jurisdiction may find adequate for their respective requirements. This will allow states to employ such technologies as they may require or already have in place. Adoption of the ECIG Implementation Guide will go a long ways to insure the interoperability of different equipment, vendors and distribution technologies.

B. Support for incorporation of the ECIG Implementation Guide.

1. We strongly support the amendment of §11.56 to require conversion of CAP into SAME in accordance with the EAS-CAP Industry Group's (ECIG) ECIG Implementation Guide, v1.0.

Monroe Electronics believes that open standards are essential to creating and maintaining a competitive marketplace, which in turn establishes a cost efficient ecosystem for the industry. Openness as developed by the EAS-CAP Industry Group (ECIG) ensures a large number of equipment choices based on high levels of interoperability and competition. Finally, open standards reflect a broad set of market requirements which ensures robust feature development for the industry.

The Commission has sought comment on certification of CAP EAS equipment, and whether it should incorporate the ECIG EAS-CAP Implementation Guidelines. To ensure high levels of data interoperability, Monroe Electronics supports the ECIG guidelines, and recommends the Commission adopt them in its rulemaking.

We observe that while the Commission feels it inappropriate to incorporate the FEMA IPAWS Conformity Assessment process, we point out that the assessment of CAP EAS encoder-decoders included rigorous and stringent testing to the details of the EAS-CAP Implementation Guide, including output to Part 11 compliant protocol[1]

Monroe Electronics supports the use of certification and conformity testing to existing Part 11 requirements as well as ECIG CAP-to-EAS Implementation Guidelines, which for example could incorporate the testing of CAP EAS encoder-decoders at Eastern Kentucky University on behalf of FEMA IPAWS for EAS CAP equipment.

[1] However, we do observe that there were differences in the testing approach applied to intermediary devices (CAP-to-EAS converters). These differences, as detailed in these comments, make the conformity assessments of intermediary devices problematic.

2. We support the Commission's conclusion that the obligation to receive and transmit only CAP-formatted messages initiated by state governors necessitates that such CAP messages will be translated into SAME-compliant messages consistent with the CAP-to-SAME translation standard adopted for Federal CAP messages – specifically, the ECIG EAS-CAP Implementation Guide.

The ECIG EAS-CAP Implementation Guide was adopted by FEMA and utilized in IPAWS conformance testing of CAP EAS encoder/decoders. We also note that the ECIG EAS-CAP Implementation Guide was adopted via unanimous votes of both the general membership and Board of Directors of the EAS-CAP Industry Group. As such, the ECIG Implementation Guide can be seen as having widespread support across industry and government.

This specification has already been implemented in all CAP-conformant EAS encoder/decoders that have passed through IPAWS conformance testing. For example, the current CAP firmware version for all Digital Alert Systems DASDEC-II and Monroe Electronics R189 One-Net EAS encoder/decoders supports the ECIG methodology for filtering and prioritizing CAP-formatted messages initiations by state governors. All other EAS encoder/decoder manufacturers have also already followed this approach.

3. We support CSRIC's recommendation to mandate that CAP-formatted messages be broadcast only if the scope of the alert is "Public" should be adopted.

We note that CSRICS's recommendation on the Public scope of alerts is based on findings contained within the ECIG Implementation Guide, as well as the IPAWS Profile. Further, the original OASIS CAP protocol specification notes that a scope of "Public" is intended for "general dissemination to unrestricted audiences", which would be the most appropriate usage for an EAS communication.

Conversely, there may be communications that are not intended for general dissemination – such as those related to exercises, tests, simulations and training. Use of CAP messages in these scenarios could be better handed with a scope of "Restricted" ("For dissemination only to users with a known operational requirement") or "Private" (For dissemination only to specified addresses).

Non-EAS uses of CAP aside, we concur that the most appropriate scope of CAP alerts intended for public alert and warning (i.e. the Emergency Alert System) is "Public".

C. Concerns over Tentative Conclusions on Delivery of CAP EAS messaging

1. We advise the Commission may create unforeseen complications by creating overly-specific requirements that EAS Participants monitor RSS 2.0 feed(s).

While the Commission rightfully concludes, tentatively, upon the broad data standards to foster interoperability (CAP, IPAWS profile and ECIG), and is setting the overall framework and establishing minimum system guidelines, Monroe Electronics urges it to maintain a neutral stance as to specific technical solutions that may have been adopted, or are being considered, by Federal, State and local jurisdictions. Neutrality is of paramount concern in order to make this next generation network of networks a success, while avoiding inadvertent stifling of innovation, imposing requirements (tacit or otherwise) on state and local government alerting systems choices.. To that end, the Commission should issue guidelines and principles where feasible in lieu of detailed regulations that inadvertently could pose a risk of freezing technological innovation.

Respectfully, we are of the opinion that it is impractical and unrealistic for the Commission to attempt to design, for the first time, an next generation IP based CAP EAS network by codifying various specific design parameters, which may not keep pace with technological innovation, and may in fact be in conflict with system and network design choices already made by a substantial number of state governments around the United States.

Rather than attempting to manage the design choices necessary for a CAP EAS system of systems, the Commission would be best served by leveraging the experience and resources of systems that are in many areas already under development or actually in operation.

The Commission's Third Further Notice indicates, among other tentative decisions, that alerting messages should be made available via RSS 2.0 feed. **As a primary concern, this tentative decision may already be not consistent with FEMA's IPAWS own decision to deploy an ATOM[2] web feed, rather than RSS 2.0.**

Secondly, such a decision by the Commission would implicitly create a mandate on specific features and requirements of CAP origination systems used, purchased and

[2] The Atom Syndication Format is an XML language used for web feeds, developed as an alternative to RSS, while the Atom Publishing Protocol (AtomPub or APP) is a simple HTTP-based protocol for creating and updating web resources. The Atom syndication format was published as an Internet Engineering Task Force (IETF) proposed standard in RFC 4287 (December 2005), and the Atom Publishing Protocol was published as RFC 5023 (October 2007).

maintained by State, county, local, territorial and tribal emergency management and public safety agencies.

This decision breaks with a tradition of Commission policy preferring technological neutrality over heavily prescriptive rules that pick technology winners and losers. We encourage the Commission to reflect on its own recognition that rules should be as "technologically neutral as possible … to avoid hindering or precluding future innovative technological developments."[3] In these public safety-related orders, the Commission has mandated a particular result – such as the delivery of E911 location information or the delivery of emergency mobile alerts.

The Commission argues that use of the RSS 2.0 methodology would provide a common method to be shared by the FEMA IPAWS systems, as well as state systems. As stated above, this is a problematic argument, since FEMA IPAWS itself has recently provided briefings to industry that is now be pursuing an ATOM web feed strategy. We also observe that this line of reasoning presents several challenges, including an implicit requirement for state and local authorities to redesign or recontract their existing CAP-based systems, which in a substantial number of cases includes combinations of satellite and Internet-based distribution. We also observe that it would be possible for states with existing CAP networks to originate and disseminate a standards conformant CAP gubernatorial message over existing IP based transmission media, without resort to a redesign to accommodate a less robust ATOM or RSS feed. We further observe that there is little technical impediment for these state and local CAP alerting systems to ingest ("pull") a FEMA CAP XML message (whether made available via RSS or ATOM), and subsequently distribute (via push or pull technologies) that same message through state IP relay networks.

Again, we urge the Commission to refrain from delving into detailed prescriptive technical decisions, as the technology of CAP EAS in general and FEMA's IPAWS in specific are dynamic. In addition to FEMA's recent indication to make CAP EAS messaging available via ATOM rather than RSS 2.0, FEMA has also indicated that it will make use of a digital signature, the corresponding key to which will be made available either to users (EAS Participants) and/or manufacturers of CAP EAS equipment that has successfully passed their IPAWS Conformity Assessment (IPAWS Conformity Assessment) process. Because details of that security/authentication measure have not yet been released to industry, we observe that detailed technical decisions are premature at this time in the context of the proposed rulemaking.

[3] Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010, First Report and Order and Third Notice of Proposed Rulemaking, 14 FCC Rcd 152 ¶ 106 (1998).

Further, we observe that the inclusion of detailed technical requirements in this area may pose additional requirements on the Commission itself. For example, in addition to the digital signature issue, FEMA has also indicated that it is evaluating possible unique identifier (such as username/password) combinations that could be required of IPAWS conformant CAP EAS equipment. While this would require a relatively modest software update for CAP EAS equipment, we also observe that this might also entail additional rulemakings and revisions of Part 11, in order to accommodate future evolution and innovation in the IPAWS system.

2. We note that most – if not all – certified and conformed CAP EAS equipment can accommodate additional technical standards covering delivery of CAP-formatted messages to EAS Participants over additional platforms, such as satellite systems.

Based on what we already know of existing and planned state and local CAP systems, we cannot help but note a contradiction in the Commission's stance that the language in the Second R&O was "was intended to put EAS Participants on notice that, should FEMA adopt technical standards covering delivery of CAP-formatted messages to EAS Participants over specific platforms, such as satellite systems, EAS Participants would ultimately need to configure their systems to be able to interface with such systems to meet their existing obligation to process CAP-formatted messages." While putting EAS participants on notice that they may need to respond to future delivery mechanism choices from FEMA, by pushing a mandate on RSS dissemination for the gubernatorial alert message, the Commission appears to be overruling – or at least trivializing – the CAP EAS delivery choices of state and local jurisdictions.

3. We do not believe that EAS Participants will "be required to deploy multiple variations of EAS equipment to meet their basic CAP-related obligations," and rather find that state and local CAP systems are seeking to leverage the same data standards adopted by FEMA's IPAWS.

We find the assumption faulty that "while FEMA has adopted one set of CAP standards to implement federal CAP processing via its IPAWS system, it seems entirely possible that a given state could adopt a different set of CAP standards for its state CAP alerting system."

Whether or not a state deploys a CAP-based system that does – or does not interface with IPAWS - we strongly are of the opinion that the same equipment required for IPAWS would satisfy the requirements of all knows state CAP initiatives. As case in point, the Digital Alert Systems DASDEC and Monroe R189 One-Net will interface with FEMA IPAWS, and both FCC certified CAP EAS encoder-decoders already support the interfaces for CAP systems deployed (or contemplated) in Alaska, California, Delaware, the District of Columbia, Florida, Georgia, Idaho, Illinois, Indiana, Maryland, Massachusetts, Michigan, Missouri, New York, North Carolina, Pennsylvania, South

Carolina, Virginia, Washington, and elsewhere. We expect much to be the case among other manufacturers of EAS equipment, if they desire to remain competitive in the marketplace.

We respectfully remind the Commission that CAP EAS equipment is capable of supporting a variety of interpretations of CAP, whether it be CAP v1.0 or CAP. v1.1 .or CAP v1.2, or whether that means a message that adheres to the IPAWS profile or not. So long as a message adheres to the CAP standard, CAP EAS devices should be able to handle that message. On the other hand, we also remind the Commission that all CAP conformant manufacturers of CAP EAS equipment have adopted the ECIG Implementation Guide, which provides a common basis for exchange and processing of CAP messaging intended for EAS, whether or not it strictly adheres to the IPAWS profile.

The use of slightly varying data standards does NOT mean that EAS Participants will be required to deploy multiple variations of EAS equipment. So long as messaging conforms to the current core CAP standards (v1.0 and higher), manufacturers will be readily capable of accommodating multiple CAP messaging systems.

Further, we make note of the ability all CAP EAS equipment, known to us, to be able to handle not only variations in CAP messages, but also the ability to handle "push" and "pull" systems on existing platforms. The Digital Alert Systems DASDEC and the Monroe Electronics One-Net, again for example, natively support all CAP EAS systems currently deployed, including NY Alert (New York), MyStateUSA (Idaho and Washington), EDIS (California), and Comlabs EMnet (in use in more than 14 states). These systems involve different delivery methodologies (push and pull) and delivery technologies (Internet, satellite and other IP distribution systems). Support for these various methodologies and technologies should not pose a significant burden for the EAS equipment manufacturer or the EAS Participant, either economically, operationally or logistically.

D. Concerns Regarding Part 11 EAS Certification

We note that known EAS encoder-decoders and EAS decoders that have integrated CAP functionality are also FCC certified. Specifically, the FCC certified portions of these devices have not in any way been altered with the addition of CAP reception and processing capabilities. For these reasons, we suggest the Commission may safely rely on the existing certifications these devices hold for Part 11 compliance.

We urge the Commission to amend §11.34 to add a provision for FCC certification of intermediary devices, in line with current provisions for FCC certification of current EAS devices. If uncertified intermediary CAP-to-EAS encoders meet the specifications under § 11.32, and are intended for use in an EAS Participant site for EAS (as described under §

11.11), then we think it advisable that they must be type Certified by the FCC as required under § 11.34. If uncertified CAP-to-EAS encoders do not meet all the specifications under §11.32, then they should not receive FCC certification, and should not be used for EAS.

Intermediary devices that convert CAP to EAS are not merely radio or data receivers. Rather these devices perform a critical function if not done correctly could put the public at risk. Further, we note that certification of intermediary devices that convert CAP messages to EAS protocol (SAME) is not currently provided by any governmental entity. Therefore, we suggest that it is necessary and appropriate that FCC perform its customary and statutory role in EAS certification relating to intermediary devices.

We again suggest that it is necessary, appropriate and essential for the FCC to take up the role of certification of intermediary CAP-to-EAS devices. There is currently no certification or testing process to assure that the CAP-to-EAS encoding functions in these new intermediary devices is performed with for Part 11 compliance. On the other hand, integrated CAP EAS encoder-decoders and CAP EAS decoders already possess Part 11 certifications for the EAS-protocol functions of the devices.[4] The ECIG Recommendations for a CAP EAS Implementation Guide (v1.0) should be utilized as the baseline for CAP-to-EAS message translation.

Based on this discussion, we remain urge the Commission to ensure that intermediary devices that encode CAP to EAS protocol will not be allowed to circumvent the requirement of FCC certification.

1. We recommend that the Commission extend existing Part 11 certification requirements to any equipment that creates EAS protocol tones from a CAP-formatted message, and that this requirement should apply to both EAS encoder/decoders, as well as intermediary devices. We further recommend that the Commission incorporate the IPAWS CAP conformance testing of EAS encoder/decoders, as a complete testing of CAP conformity. However, we caution the Commission to reconsider whether IPAWS CAP conformance testing of intermediary devices can be relied upon, since that testing omitted several key portions of the IPAWS CAP profile and ECIG CAP-EAS Implementation Guide.

We observe that all EAS encoder/decoders that have successfully completed IPAWS conformance testing also hold FCC Part 11 certification. Existing Part 11 type certification should suffice, to the extent that the addition CAP capabilities in a given

[4] The CAP functionality in integrated encoder-decoders does not in any way alter the previously certified functions of the EAS encoder-decoder. Encoder of CAP messages into EAS (SAME) is adequately covered by these existing certifications.

piece of equipment has not require internal modification of the device that would substantially change the original configuration as originally FCC type certified. That is, if the CAP processing element can be added to next-generation EAS equipment without requiring modification of components tested for Part 11 compliance.

The augmentation of an existing Part 11 certified device (EAS encoder/decoder) with internal (on-board) CAP capability can be demonstrated via the FEMA IPAWS Conformity Assessment Test Results accompanied by a Suppliers Declaration of Conformity. . While acknowledging that the Commission does not feel it appropriate to incorporate that test process per se, we observe that the IPAWS Conformity Assessment process assesses conformance by EAS encoder/decoders to the CAP v1.2 standard and the ECIG Implementation Guidelines. The IPAWS Conformity Assessment process used the ECIG CAP-to-EAS Implementation Guide as a main component and benchmark.[5] Therefore, if device has successfully completed those test parameters, then there can be a level of assurance that the EAS device in question does adequately conform to the ECIG guidelines.

As a case in points, both the Digital Alert Systems DASDEC and Monroe-R189 One-Net successfully completed IPAWS Conformity Assessment testing, and conform strictly to the CAP v1.2 protocol and ECIG Implementation Guide. A copy of the test results for that EAS equipment has been included appendix B.

However, we must caution the commission that the IPAWS Conformity Assessment process contains a number of omissions in regards to the evaluation of intermediary devices (CAP converters) that severely impair the usefulness of the conformity assessments of those devices. Specifically, the test cases used in the conformity assessment process omitted evaluation of the ability to process a CAP formatted governors must carry message in intermediary devices, while EAS encoder-decoders were tested in regards to that functionality. As a result, we take serious exception to any claim on the basis of these conformity assessments whether an intermediary device (CAP converter) fully adheres to the ECIG CAP-to-EAS Implementation Guide v1.0.

[5]See *Integrated Public Alert and Warning System (IPAWS) Conformity Assessment (CA) Program Guide* (December 2010). As noted in the Program Description section of the document "The IPAWS CA Program provides an objective test of commercial and government software and hardware products (e.g., Encoder/Decoders) to assist in the implementation of IPAWS. Testing activities are designed to provide FEMA an objective process to verify conformance of software and hardware solutions, including EAS products as well as other alert and warning products that may not be bound by FCC Part 11 rules. A sub-purpose is to indicate results with respect to other industry recommendations such as the CAP EAS Implementation Guide."

If a given piece of EAS equipment is to be modified with the addition of an external CAP processing element, there are several additional considerations. If that external CAP processing element performs any function covered by Part 11 regulation, then that external CAP element should stand for FCC certification in and of itself. For example, if an external CAP processing element functions by producing (that is encoding) EAS protocol for consumption by and EAS decoder, then that would certainly appear to fall directly under § 11.33. Further §11.33 points to the requirement in §11.34 for type certification of this type of EAS encoding device.

2. We recommend that the Commission should incorporate the ECIG CAP-EAS Implementation Guide as a baseline to ascertain compliance with respect to CAP functionality.

As noted above, to the extent that FEMA IPAWS Conformance testing for EAS encoder/decoders represents a full testing of that Implementation Guide, the results of that testing should be accepted in tandem with an FCC Part 11 type certification for the EAS encoding and/or decoding functions of the device. These requirements should extend to CAP EAS encoder/decoders, CAP EAS decoders, and intermediary devices.

3. As noted, we feel the Commission would be well served by certifying equipment that has documented conformance with the ECIG Implementation Guide, and further feel that conformance testing for the ECIG Implementation Guide could be implemented achieved through acceptance of testing results from a bona fide third party process of facility.

For example, conformance by EAS encoder/decoders with the ECIG Implementation guide can be demonstrated via the successful completion for the IPAWS Conformity Assessment process, insofar as valid Test Results and a Suppliers Declaration of Conformity (SDOC) can be furnished by the equipment manufacturer. That SDOC and Test Results document could be submitted directly to the FCC as evidence of ECIG Implementation Guide conformance.

However, we must advise the Commission that – separate from the test process of EAS encoder/decoders – the IPAWS Conformity Assessment for CAP converters (a/k/a intermediary devices) was marked by such fundamental and serious omissions that those tests cannot be relied upon to demonstrate full conformance with the ECIG Implementation Guide or CAP standard.

4. We believe that the current FCC certification process is sufficient for the EAS-protocol (SAME) encoding/decoding functions. In conjunction with the test results described above for EAS encoder/decoders, the Commission should be able to have a definitive assurance of EAS and CAP compliance.

E. Issues concerning "intermediary" devices

1. We are seriously concerned over the misperception of intermediary devices, and caution that the actual functionality of these devices would seem to be inconsistent with Part 11 rules. At a minimum, we recommend that the Commission require that any such devices be subject to the core certification criteria of other EAS equipment, including Part 11 and Part 15 certification.

"Intermediary devices" may be defined as those which receive CAP messages and encode the content into to EAS protocol tones. These EAS protocol tones are used as a monitoring source for a legacy EAS unit that would still be left in place. It is critical to note that intermediary devices do not merely feed an audio output to an audio input of an EAS encoder-decoder.

Rather, intermediary devices receive CAP messages and actively encode them into EAS protocol format. Further, we are aware of at least one intermediary device which apparently claims to be able to place a CAP-formatted gubernatorial message on air via use of a relay cable (possibly bypassing the legacy EAS encoder-decoder

By definition, these devices are actually uncertified EAS encoders. There is therefore a critical distinction between equipment that is FCC certified (Part 11 and Part 15 compliant) and intermediary equipment that is performing the same fundamental role, but do not have the required FCC certifications.

We suggest that uncertified CAP-to-EAS encoders are problematic in light of requirements and obligations established in CFR Title 47, Part 11. There are several specific subsections within Part 11 which call into question whether Uncertified CAP-to-EAS encoders meet the FCC's requirements of EAS participants (including cable operations) and vendors of EAS systems.

Specifically:

- The encoding of the EAS protocol (AFSK tones) from CAP formatted alerts clearly falls under the requirements set forth in §11.32 "EAS Encoder". Any devices (hardware and/or software) performing the action of encoding EAS protocol fall under §11.32.
- §11.32 provides the specifications for all EAS Encoders. One problem for uncertified CAP-to-EAS encoders is that they mimic many of the key specifications of an EAS encoder, but pretend not to be subject to any required FCC certification.
- Basically this is a case of uncertified CAP-to-EAS encoders trying to have their cake and eat it too. Uncertified CAP-to-EAS encoders are mimicking the role of an EAS encoder, but circumventing the certification requirement. The certification

> requirement is plainly set forth in §11.34 "Acceptability of the Equipment", under which an EAS Encoder used for generating the EAS codes and the Attention Signal **must be Certified** in accordance with the procedures specified in Part 11.

The point of these Part 11 requirements are not trivial. They are intended to assure the correct interoperability of these devices, produced by different vendors, to produce a level of assurance that this alerting system would carry out its duties in the face of a national emergency.

This certification issue has been recognized by several key parties. A key FCC advisory council (the Communications, Security, Reliability and Interoperability Council, or "CSRIC") advised the Commission that uncertified CAP-to-EAS encoders should be FCC certified. In an expression of widespread industry understanding, the National Cable Television Association (NCTA), Society of Cable Television Engineers (SCTE), National Association of Broadcasters, Society of Broadcast Engineers as well as other broadcast and cable organizations filed comments with the FCC supporting the CSRIC recommendations.

To summarize, if uncertified CAP-to-EAS encoders meet the specifications under §11.32, and are intended for use in an EAS Participant site for EAS (as described under §11.11), then we feel that they must be type Certified by the FCC as required under §11.34(a). If uncertified CAP-to-EAS encoders do not meet all the specifications under §11.32, then they should not receive FCC certification, and should not be used for EAS.

2. We concur that the minimum requirements for decoders in section §11.33(a) should include the capability to decode CAP-formatted messages and convert them into SAME protocol-compliant messages, as defined in the ECIG CAP-to-EAS Implementation Guide.

However, we are not convinced that this requirement can be fully met through the deployment of an intermediary device, while this requirement can be fully met through integrated CAP-EAS encoder-decoders.

In regards to the use of intermediary devices, if the intermediary device itself decodes a CAP message and converts to SAME protocol compliant messages (for consumption by an EAS decoder), then that intermediary device would appear to clearly fall under the requirements of § 11.32(a), (b), (c) and (d), as well as § 11.34(a).

3. Regarding the revision of the tables in § 11.11, we urge the Commission that if a footnote is added to the "EAS decoder" entries, it should be limited to an indication that EAS Participants may elect to meet their obligation to receive and translate CAP-formatted messages via an appropriately FCC certified and CAP conformant technology. Rather, we suggest that the Commission should eliminate the tables in

section § 11.11, and in their place simply require EAS participants to require a CAP EAS encoder-decoder or CAP EAS decoder.

Respectfully, we must raise a question as to why language is being contemplated on "intermediary devices" which gives the impression of favoring a specific technology – even specific manufacturers by inference – rather than taking a more neutral stance. We note that the references to intermediary devices should at a minimum have been accompanied by references to integrated CAP-EAS encoder-decoders (and CAP-EAS decoders). This omission is particularly problematic considering that the vast majority of those who have already acquired CAP EAS gear have acquired CAP-EAS encoder-decoders or CAP-EAS decoders. Regardless of whether the obligation is met via integrated CAP EAS encoder/decoder or via "intermediary device" the requirement should still stand that any such approach must meet all Part 11 certification requirements.

4. Again, we suggest that the Commission should eliminate the tables in section §11.11 and require all EAS participants to use a common EAS protocol and Common Alerting Protocol (CAP) to send and receive emergency alerts by means of a CAP EAS encoder-decoder or CAP EAS decoder.Intermediary devices should be classified as stand-alone devices as opposed to modifications to existing equipment.

We note again that in regards to the use of intermediary devices, if the intermediary device itself decodes a CAP message and converts to SAME protocol compliant messages (for consumption by an EAS decoder), then that intermediary device would appear to clearly fall under the requirements of §11.32(a), (b), (c) and (d), as well as §11.34(a).

F. Support for maintaining the September 30, 2011 deadline for CAP Compliance

1. We believe that the September 30, 2011 deadline for CAP-compliance set forth in the Waiver Order is sufficient, and any extension or modification could have significant repercussions for EAS stakeholders.

We feel that the September 30, 2011 deadline for CAP compliance is more than sufficient based on the following reasons:

- Information on the relevant standards and requirements have been available from FEMA and industry groups including the EAS-CAP Industry Group for months, and in cases for years.

- Vendors that are IPAWS conformant are already listed on FEMA's www.rkb.us website. All vendors listed as conformant on that website also happen to be manufacturers of FCC certified equipment.

- There are few, if any, outstanding that we feel could not be resolved via software/firmware update, which may easily be accommodated by CAP EAS equipment in the field.

We would respectfully make mention of the likelihood that a number of EAS Participants are procrastinating and delaying acquisition of CAP-compliant EAS equipment due to prior CAP deadline extension, and perception that they may be additional deadline extensions.

In light of the foregoing, we observe that many of the additional trigger points suggested by CSRIC have already been met, in one form or another.

We suggest to the Commission that it is an appropriate and necessary objective to lay the technology foundation today – including installation of certified and conformed EAS equipment – so that the basis for further development, testing and deployment of next generation EAS can be accomplished. Government and industry need to establish the first steps now, so that the system can be adjusted, expanded and refined as needed by respective Federal, state and local jurisdictions. We remind the Commission that such adjustments and refinements in next generation EAS will principally involve software/firmware upgrades that can be readily accommodated after the equipment is in the field (in fact man of the updates may only be discoverable after the system is fielded).

2. We believe that a suitable certification regime is currently in place to permit marketing and deployment of CAP-compliant EAS equipment (whether under the current or amended rules.

CAP-compliant EAS equipment has already been designed, certified and marketed by numerous vendors. We believe a suitable certification regime is already is in place. Numerous vendors have already designed, certified and marketed CAP-compliant EAS equipment. We also observe that a very significant portion of EAS Participants have already purchased or issued contracts to purchase CAP-compliant EAS equipment.

3. We do not believe any additional extension of the September 30, 2011 CAP compliance deadline is necessary or warranted, given the good faith efforts of the EAS manufacturing industry, as well as the EAS participants, to develop, market, acquire, deploy, and test the new equipment.

We are unclear as to the real benefits of any further extension(s) of the CAP deadline. CAP EAS equipment is currently manufactured by a number of vendors, meeting FCC

Part 11, FEMA, OASIS and ECIG specifications. Relevant certifications and conformity assessments have been completed by these manufacturers.

In addition, a significant number of EAS participants have already acquired, deployed and tested this equipment. A significant portion of EAS participants have already invested the resources in acquiring CAP EAS equipment, planning CAP upgrades, and coordinating downstream enhancements to accommodate CAP, well in advance of the 30 September CAP compliance deadline. In fact, broadcast operations of every size across the nation have already contracted (and in many cases deployed) CAP EAS encoder-decoders, including such companies as 4 Points Media Group, Belo Broadcasting, Clear Channel Communications, Fusion Communications, Hearst Television, Qantum Communications, Three Angels Broadcasting Network, Townsquare Media, and so forth.

We feel that the burden caused by further delays and extensions would be felt across the industry, with potentially serious impacts on some industry segments. We caution the Commission of likelihood of unintended consequences that would be caused by additional delays and extensions.

- We are concerned that there would likely be a series of unintended costs and consequences to EAS participants by continuing the uncertainty of a reliable CAP deadline.

- The would likely be unintended costs and consequences to Federal state and local government agencies, including any potential impact on the FEMA IPAWS program, as well as state and local CAP initiatives that are currently planning or investigating interconnectivity with IPAWS for purposes of both advanced EAS and access to CMAS/PLAN.

- There would almost certainly be unintended costs and consequences to EAS equipment manufacturers by removing essential elements of predictability in the market and in their ability to plan their supply chain. EAS manufacturers have by and large organized themselves around the existing 30 September deadline. They have acquired significant inventories of components to meet projected demand leading up to that deadline. They have scaled their operations, including increasing staff and repurposing employees, also for the purposes of meeting projected demand in advance of the existing CAP compliance deadline. Additional delays and extensions could be seriously disruptive to many of the operations of these firms, which have been cooperating to date with Government mandates.

- Finally, there would be unintended costs and consequences to the public, by denying the availability of next generation CAP services, and potentially delaying

further innovation for integrated public warning systems including services for the disabled, multilingual and other specialized populations.

The Commission asks whether additional time is needed from the effective date of a suitable certification regime for CAP-enabled EAS equipment for manufacturers to certify and begin to market CAP-compliant EAS equipment. We are concerned about this question and approach. Firstly, EAS manufacturers are already subject to Part 11 EAS certification requirements. Secondly, EAS encoder/decoder manufacturers have been subjected to a CAP conformity assessment process organized the Department of Homeland Security's FEMA. We believe that subjecting EAS manufacturers to an additional CAP certification regime would be redundant to that already organized by FEMA for EAS encoder/decoders. Further, we believe that such an additional test regime would pose an unnecessary and costly burden on manufacturers that have already made good faith efforts to work with the Government in assuring the CAP conformance of their equipment. To this end, we believe that sufficient certification exists to the extent that an EAS encoder/decoder (1) holds FCC certification for the Part 11 (EAS SAME) related functions of the device, and (2) holds a successful FEMA IPAWS CAP Conformity Test Results Report, with accompanying Suppliers Declaration of Conformity.

We also remind the Commission that EAS Participants have been required since the date of the Second Report and Order to acquire CAP EAS equipment. Many EAS Participants have complied with the Commissions requirement by purchasing and installing CAP EAS equipment. Most EAS participants have looked to the individual statement from (1) on the one hand, the FCC to acquire the ability to accept CAP messages, and (2) on the other hand, DHS FEMA to refer to products that have completed the IPAWS CAP process (as posted on the FEMA Responders Knowledge Base).

With that in mind, it would seem that the creation of an additional compliance regime would create redundancy, confusion and unnecessary delays, and would potentially be materially injurious to manufacturers of EAS equipment. Therefore, we urge the Commission to consider that any extension to the CAP compliance deadline could have dramatic negative impacts to the overall transition to CAP.

4. We believe that most extenuating circumstances can be addressed on a case-by-case basis through the waiver process, such as the time required for EAS Participants located in rural or underserved areas to obtain IP connectivity.

It may well be that case that waivers may be appropriate in selected cases, such as for genuine economic hardship, or the physical unavailability of IP connectivity. We are hopeful, given the FCC's efforts on behalf of the National Broadband Plan, that the availability of broadband connectivity will steadily increase across the country. We also take note of the efforts of some smaller broadcasters to already obtain satellite IP

connectivity, in the absence of traditional IP connections. Regardless, of the availability of IP connectivity, all EAS participants should be encouraged to implement the required CAP EAS equipment by the established deadline, to put in a state of readiness for when IP connectivity becomes available. The physical unavailability of IP connectivity in selected cases should not remove the responsibility of the EAS Participant to put the basic equipment into place to meet the obligation of internally being ready to accept CAP messaging.

G. Comments Regarding the gubernatorial message

1. We agree with the tentative conclusion that the obligation to receive and transmit CAP-formatted messages initiated by state governors applies only to the extent that such CAP messages have been formatted using the CAP standards adopted by FEMA – specifically, OASIS CAP Standard v1.2 and CAP v1.2 USA IPAWS Profile v1.0. However, we also strongly recommend the addition of the essential CAP-to-EAS formatting requirements of the ECIG CAP EAS Implementation Guide v1.0.

We urge the commission to adopt the CAP formatting requirements further specified within the EAS CAP Industry Groups' Implementation Guidelines, which has also been adopted by FEMA for Federal CAP messages. The ECIG CAP-to-EAS Implementation Guidelines were unanimously adopted by the ECIG membership, which represents virtually all EAS equipment manufacturers, as well as major CAP alert origination systems.[6]

The ECIG EAS-CAP Implementation Guide provides a formula for formatting gubernatorial messages in CAP. See Section 3.4.1.7 "Governors Must Carry": "Messages for which the Governor's … authority is invoked SHALL be marked by the inclusion of an additional CAP <info><parameter> block with a <valueName> of "EAS-Must-Carry" and a <value>of "True." If this parameter is present and the value is TRUE, then the CAP message has come from a state governor's office (or designee) and the EAS system must place the message on air according to the rules defined in the applicable State plan.

We note that the ECIG CAP-to-EAS Implementation Guide methodology was utilized as a key element in defining testing parameters for effective processing of a gubernatorial message by a CAP-enabled device for the IPAWS Conformity Assessment process. Parenthetically, we note that the ECIG CAP-to-EAS Implementation Guide was voted

[6] ECIG members representing CAP origination systems providers provide CAP EAS capabilities in over 18 states across the nation.

upon and accepted unanimously by the membership of ECIG, which included virtually all representatives of the EAS manufacturing industry.

2. We do not feel that a new origination and/or event code would be warranted to fully implement the obligation of EAS Participants to process CAP formatted messages initiated by state governors.

The use of a new origination or event code would at least superfluous – if not outright inconsistent - with the ECIG Implementation Guidelines, as adopted by FEMA. The ECIG guidelines were developed to help assure that alerts are issued about known event types with a gubernatorial priority, and were adopted with unanimous agreement among ECIG members, representing the vast majority of EAS manufacturers.

Conversely, the additional of a new event code would add very little to the capabilities already specified in the ECIG CAP-to-EAS Implementation Guide. To contrary, addition of a new event code could create considerable confusion, message ambiguity, and incompatibility with the IPAWS system.

Adding a new event or origination code would add ambiguity, as the textual display of such a message would (1) contain little if any effective information about the actual event, and (2) the audio would likely substantially differ from the textual portion, particularly in the case where legacy EAS equipment may somehow still be supported. This also raises the difficulty of making emergency communication information equally available for those who rely on textual displays rather than audio.

Issuance of an alert using a new gubernatorial code for legacy EAS alongside a CAP-conformant gubernatorial alert will inevitably lead to confusion over multiple messages with differing audio and textual information, not only between the two alerts, but even within each alert itself.

Given the foregoing, we urge Commission to maintain the symmetry established by the ECIG Implementation Guidelines, by enabling an override (mandatory) capability for alerts of any event type, should a governor (or designee) feel that a given alert is warranted for such priority treatment. We also note that all vendors represented in ECIG voted unanimously to adopt the ECIG CAP-to-EAS Implementation Guide, including the gubernatorial alert capability specified within the EGIC guidelines. We further note that all EAS encoder/decoders were stringently tested during the ECIG CAP-to-EAS Implementation Guide to the ECIG gubernatorial alert capability. Digital Alert Systems, Monroe Electronics, and other manufacturers of CAP EAS encoder-decoders have all successfully completed the IPAWS Conformity Assessment process, including test of the industry approved and FEMA adopted ECIG gubernatorial alert methodology.

3. We agree with the tentative conclusion that the geo-targeting requirement associated with mandatory state governor alerts shall be defined, at least for the time being, by the location provisions in the EAS Protocol.

4. We agree that the CAP gubernatorial message must reset after the two minute interval, and §§33(a)(9) remains relevant as currently written.

If the Commission adopts the ECIG EAS-CAP implementation guidelines, as it has tentatively concluded, this methodology would have the effect of "tagging" a CAP EAS gubernatorial message with a CAP parameter which would direct the CAP EAS encoder/decoder to override the device Originator and Event Code filtering for automatic forwarding. Local device Location Code filters, duplicate alert prevention, and the alert duration limit will still apply. The CAP gubernatorial parameter is consistent with any existing EAS/SAME event code, and does not impact the alert duration limit. As such, §11.33(a)(9) remains relevant as written.

5. We suggest that it may be useful to provide, in section §11.44, gubernatorial CAP-formatted messages with priority over local EAS messages. However, we suggest that additional guidelines may be useful to further define the circumstances under which a priority gubernatorial EAS message is warranted.

We can primarily speak to the technical feasibility in the DASDEC and One-Net. Both FCC-certified units can allow gubernatorial CAP-formatted messages with priority over local EAS messages. At the same time, we suggest that the "threshold" for tagging an EAS message with the gubernatorial priority needs to be further defined for both originators and receivers of such messages.

As discussed previously, the ECIG EAS-CAP Implementation Guide a gubernatorial message only overrides the device Originator and Event Code filtering for automatic forwarding. Local device Location Code filters, duplicate alert prevention, and the alert duration limit will still apply.[7]

6. We suggest that §11.51(m) should be amended to incorporate the obligation to process CAP-formatted messages initiated by state governors.

Specifically, we recommend a new subsection numbering under which the current §11.51(m) should be renumbered §11.51(m)(1), and a new §11.51(m)(2) is added to

[7] The ECIG EAS-CAP Implementation Guide provides a formula for formatting gubernatorial messages in CAP. See Section 3.4.1.7 "Governors Must Carry": "Messages for which the Governor's … authority is invoked SHALL be marked by the inclusion of an additional CAP <info><parameter> block with a <valueName> of "EAS-Must-Carry" and a <value>of "True." If this parameter is present and the value is TRUE, then the CAP message has come from a state governor's office (or designee) and the EAS system must place the message on air according to the rules defined in the applicable State plan.

define the obligation to process CAP-formatted messages initiated by state governors based on an approved state EAS plan.:

> "(m)(2) EAS Participants are required to transmit all received CAP-formatted, ECIG conformant EAS messages in which the gubernatorial CAP parameter exists, and the header code may contains any valid Event, and when the accompanying location codes include their State or State/county. These EAS messages shall be retransmitted unchanged except for the LLLLLLLL-code which identifies the EAS Participant retransmitting the message. See § 11.31(c). EAS messages may be transmitted automatically or manually."

H. EAN

1. We concur that the Emergency Action Termination (EAT) should be eliminated and replaced where necessary with the EOM in the Part 11 rules.

There are actually two issues here – first the clarification of the usage of an EOM to end EAT alert transmissions, and second the role (if any) of the EAT alert message. As for the first, we suggest that Part 11 rules should be clarified to specify that the SAME-formatted EAN alert is ended with an EOM transmission.

As for the second, we note that the EAN and the EAT are separate and distinct messages, each closed by their own EOM. The overall role of the Emergency Action Termination has to date not been sufficiently clarified. Further, fundamental characteristics of the EAT have likewise remain unclear, including the length of the audio message (limited to two minutes, or unlimited audio).

While we, of course, defer to national authorities to define their own concept of operations for the EAN and EAT, we suggest that the EAT is sufficiently redundant to an EAN as to warrant elimination in the list of authorized EAS codes. Further, due to the insufficient definition of the EAT, and potential for conflicting interpretations of usage of the EAT in EAS equipment (as well as other related equipment used by EAS participants), we recommend that the EAT event code be eliminated.

2. As to the question of whether 11.53 should be deleted, or revised to incorporate CAP-formatted EAN messages, we observe that FEMA IPAWS has not yet issued requirements for a CAP-formatted EAN message. Since it is anticipated that EAN messages will be delivered over the current legacy EAS system for the foreseeable future, it would seem that §11.53 remains relevant in its current form.

3. We concur that section §11.33(a)(11) could be updated to specify that a CAP-formatted message containing a header code with the EAN event code received through a non-audio input must override all other messages.

However, as noted above, this would be reflective of a future capability, as FEMA IPAWS currently has not provided requirements for a CAP-formatted EAN message, and such EAN communications are likely to be delivered via the PEP system as legacy EAS communications for the time being.

4. We feel that the contents of section § 11.13 - the definitions for Emergency Action Notification (EAN) and Emergency Action Termination (EAT) – could be moved to §11.2, and restated under §11.31.

Should the Commission decide to eliminate the redundant EAT event code, then the contents of §11.13(b) can be deleted entirely. Should the Commission elect to retain the EAT event code, the definition contained under §11.13(b) must be amended. As currently stated, the working under §11.13(b) confuses an EAT message with the End of Message (EOM) signal terminating an EAN message.

As defined in the current section §11.31, the EAN and EAT are separate event codes, each with their own EOM signal. As such, the EAT is not the notice to all EAS Participants and to the general public that the EAN has terminated. Rather the EAT would conceivably be a notice that a national emergency has ended. Again, however, it would appear that an EAT message is superfluous to the ability to merely issue a follow-up EAN message.

I. Display of CAP alert information

1. As to whether the SAME-based protocol codes should continue to be used as the baseline for deriving the visual EAS message requirements in sections §11.51(d), (g)(3), (h)(3), and (j)(2), we note the approach taken in the ECIG EAS-CAP Implementation Guidelines.

One of the basic advantages of CAP-formatted messaging is the ability to display additional textual information beyond the SAME-based protocol codes. We suggest that the SAME-based protocol codes may be used a minimal baseline for deriving visual message requirements. We refer the Commission to the ECIG Implementation Guide, Section 3.6 “Constructing Alert Text from CAP V1.2 IPAWS v1.0 Profile for EAS

activations," which describes the method already adopted by industry and FEMA for constructing the alert display text. Also defined is a single explicit element that will provide the needed text in a single place. As recommended elsewhere in these comments to the Commission, incorporation of the ECIG Implementation Guide by the FCC would address the issue of deriving visual EAS message requirements from CAP formatted message.

J. Miscellaneous Issues

1. We suggest that that there has been confusion around the language used by CSRIC agreeing to revise section §11.51 to require EAS Participants to transmit (or "render") a CAP-compliant message.

We generally concur with the Commission's tentative conclusion that EAS encoders should be not required to encode (originate) CAP messaging, and that EAS Participants should only be required at this time to be capable of retrieving CAP-formatted Federal EAS alerts and converting them into SAME-compliant messages for transmission to the public (and, as applicable and technically feasible, encoding them in SAME for rebroadcast).

However, we suggest (as a member of the CSRIC working group drafting the recommendations), that the CSRIC recommendation for §11.32 was that EAS encoders should be capable of converting or encoding a CAP-formatted message into EAS SAME protocol output. In regards to §11.32(a), CSRIC recommended the modification of EAS encoder minimum requirements in light of the fact that EAS encoders must be capable of "rendering" a fully CAP compliant message. The usage of the term "render" in this context was that of "converting" or "encoding" a CAP message into EAS protocol output, in compliance with other Part 11 subsections. The working group did not intend for the Commission to infer that "rendering" in this instance meant "originating" or "authoring" CAP for the purposes of transmitting CAP XML content over broadcast media.

That being said, we note that the DASDEC and One-Net have successfully completed FEMA IPAWS Conformity Assessment process for both receiving AND originating CAP messages. That is, the DASDEC and One-Net have been successfully tested for (1) receiving a CAP message[8] and encoding it into EAS protocol consisted with Part 11 rules,

[8] The FEMA IPAWS Conformity Assessment process evaluated whether equipment demonstrated conformance with FEMA data specifications for the new IPAWS system, which include: the Organization for the Advancement of Structured Information Standards (OASIS) Common Alerting Protocol (CAP) v1.2 Standard, OASIS CAP v1.2 USA IPAWS Profile, and the ECIG CAP EAS Implementation Guide v1.0.

and (2) originating a CAP message, for the eventual purpose of outputting that CAP XML message to the IPAWS aggregator and/or to state and local CAP networks. While the DASDEC and One-Net can encode EAS messages and both FSK and CAP format, we don't see a need to necessarily revise §11.32 in light of these kinds of technical innovations.

As such, we observe that the structure and intent of the FEMA IPAWS conformity assessment process was in part to assess whether given equipment was capable of accepting a properly constructed CAP message, **and encoding that message into EAS protocol output consisted with Part 11 definitions**.

2. We strongly recommend that the input and output configuration requirements in sections §11.32(a)(2) and (a)(3), and sections §11.33(a)(1) and (a)(7), should be modified to include a requirement for *at least one* Ethernet port.

There is no practical reason to make a limitation to only one single Ethernet port, as suggested in the phraseology in the FNPRM. Quite to the contrary, many EAS participants have found multiple Ethernet ports both useful and necessary in their operations. For this reason, we strongly recommend that the aforementioned configuration requirements include a requirement for ***at least one*** Ethernet port. Further, the specification of a requirement for a single Ethernet port would seem to favor one particular manufacturer, who only provides one Ethernet port, over other manufacturers, who provide multiple Ethernet ports in their CAP EAS equipment. Again, the language should be modified to include a requirement for *at least one* Ethernet port.

3. We do not agree with the elimination of existing requirements for 1200 baud RS-232C interface.

We advise the Commission that there are numerous broadcast and cable operations that current **still utilize** the RS-232C interface for various applications and services. As such, there is no need to eliminate the existing requirements for 1200 baud RS-232C interfaces. At a minimum, the revised rules should not preclude inclusion of RS-232C interface as an option.

4. We agree with the concept that section §11.33(a)(4) should be modified to require that if an alert message is derived from a CAP-formatted message, the contents of the text, assembled pursuant to ECIG Implementation Guide, should be added to the EAS device log.

5. We concur with the tentative conclusion that there is no basis for revising section §11.33(a)(10) to require processing of CAP-formatted message by default when duplicate messages are received in both the EAS Protocol and CAP formats if

EAS Participants are required to translate CAP-formatted messages into SAME-formatted message in conformance with the ECIG Implementation Guide.

Insofar as that when a CAP and EAS protocol message contain identical header information, there is no need to add a preference to the CAP message. The first message received should be processed, and duplicates logged.

6. We recommend that section §11.11(a) should be amended to include as a minimum requirement compliance with the CAP-related requirements in section §11.56. We also recommend that the text in the table "Analog and Digital Broadcast Stations" be amended to reflect "CAP EAS encoder" and "CAP EAS decoder". Further, the reference to "analog television broadcast stations" is obsolete and should be deleted.

7. We feel that the language of section §11.20 should be amended to provide State Relay Networks with the option of distributing EAS messages in CAP and/or legacy EAS format. Of course, only CAP alerts and/or CAP relay networks would be eligible of disseminating a gubernatorial priority message.

8. We concur with the Commission's tentative conclusion that the text of sections §11.21(a) and §11.55(a) should be revised to make clear that they apply to CAP-formatted EAS messages.

9. We disagree with the tentative conclusion that it is unnecessary to include a CAP-receiving requirement in section §11.35(a).

At a minimum, it should be specified that CAP EAS encoder/decoders fall under the same requirements of §11.35(a), (b) and (c). Further, to the extent that intermediary devices are permitted, it is unclear why they would or should be exempt from the operational readiness requirements set forth under §11.35, as their role as and EAS encoder (certified or not) would represent a critical vulnerability and potential point of failure.

10. We feel that it may make sense to revise or expand section §11.45 to accommodate CAP-formatted messages.

A possible addition to §11.45 may be the inclusion of language to the effect that no person may transmit or cause to transmit a message formatted in the Common Alerting Protocol, with the intention of activating EAS codes or an Attention Signal, or a recording or simulation thereof, in any circumstance other than in an actual National, State or Local Area emergency or authorized test of the EAS.

11. Regarding the EAS Operating Handbook, we do not feel it should be deleted, however it if is retained, the EAS Operating Handbook must be updated to correct a range of ambiguities, inconsistencies and errors.

12. We concur with the tentative conclusion that the references to the Federal Information Processing Standard (FIPS) numbers (as described by the U.S. Department of Commerce in National Institute of Standards and Technology publication FIPS PUB 6–4.FIPS number codes) in section §11.31 and §11.34(d) should be replaced by references to the American National Standards Institute (ANSI) Codes INCITS 31.200x (Formerly FIPS 6-4), Codes for the Identification of Counties and Equivalent Entities of the United States, its Possessions, and Insular Areas standard that superseded it.